CLAIMS

What is claimed is:

1. A method for prohibiting iSCSI discovery sessions, comprising:

receiving an iSCSI login request;

determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, rejecting said iSCSI login request.

2. The method of claim 1, wherein said iSCSI login request is rejected with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

3. The method of claim 1, further comprising:

declaring a session type on said iSCSI login request.

4. The method of claim 1, further comprising:

when a session type is not explicitly declared on said iSCSI login request, assuming a session type is not a discovery session and specifying a specific target.

5. An apparatus for prohibiting iSCSI discovery sessions, comprising:

means for receiving an iSCSI login request;

means for determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, means for rejecting said iSCSI login request.

6. The apparatus of claim 5, wherein said means for rejecting said iSCSI login request comprising means for rejecting said iSCSI login request with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

7. The apparatus of claim 5, further comprising means for declaring a session type on said iSCSI login request.

8. The apparatus of claim 5, further comprising:

when a session type is not explicitly declared on said iSCSI login request, means for assuming a session type is not a discovery session and means for specifying a specific target.

9. A computer-readable medium having computer-executable instructions for performing a method for prohibiting iSCSI discovery sessions, said method comprising:

receiving an iSCSI login request;

determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, rejecting said iSCSI login request.

10. The computer-readable medium of claim 9, wherein said iSCSI login request is rejected with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

11. The computer-readable medium of claim 9, wherein said method further comprising:

declaring a session type on said iSCSI login request.

12. The computer-readable medium of claim 9, wherein said method further comprising:

when a session type is not explicitly declared on said iSCSI login request, assuming a session type is not a discovery session and specifying a specific target.

13. A method for providing iSCSI target stealth operation, comprising:

providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

14. The method of claim 13, wherein said enable/disable is distributed throughout a management application.

15. The method of claim 13, wherein said warning is provided to an administrator.

16. The method of claim 13, further comprising:

when all discovery mechanisms are disabled, providing said warning to a user.

17. An apparatus for providing iSCSI target stealth operation, comprising:

means for providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, means for providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

18. The apparatus of claim 17, wherein said enable/disable is distributed throughout a management application.

19. The apparatus of claim 17, wherein said warning is provided to an administrator.

20. The apparatus of claim 17, further comprising:

when all discovery mechanisms are disabled, means for providing said warning to a user.

21. A computer-readable medium having computer-executable instructions for performing a method for providing iSCSI target stealth operation, said method comprising:

providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

22. The computer-readable medium of claim 21, wherein said enable/disable is distributed throughout a management application.

23. The computer-readable medium of claim 21, wherein said warning is provided to an administrator.

24. The computer-readable medium of claim 21, wherein said method further comprising:

when all discovery mechanisms are disabled, providing said warning to a user.